The effect of parameter uncertainty on achieved safety integrity of safety system

Ming Xu[1], Tao Chen[2,*], Xianhui Yang[1]

[1]Department of Automation, Tsinghua University, Beijing 100084, China
[2]Division of Civil, Chemical and Environmental Engineering, University of Surrey, Guildford GU2 7XH, UK

[*] Corresponding author. Tel.: +44 1483 686593; Fax: +44 1483 686581
Email: t.chen@surrey.ac.uk

Abstract

This paper introduces the concept of safety-related (SR) uncertainty and the methodology to measure SR uncertainty. SR uncertainty is concerned with the effect of parameter uncertainty on the uncertainty of system *unsafety* (defined with respect to achieved safety integrity level), which is in direct contrast to the effect on overall system uncertainty. The properties of SR uncertainty are discussed and its significance in analyzing safety systems is highlighted. The conventional global sensitivity analysis (GSA) to handle overall uncertainty is inappropriate when SR uncertainty is of interest. We present and discuss four methods to measure SR uncertainty. Three examples are used to demonstrate the effectiveness of the proposed methods in comparison with GSA.

Keywords: Safety system; Importance measure; Safety-related uncertainty; Global sensitivity analysis; Safety integrity level

1. Introduction

Dealing with uncertainty is among the major challenges for quantitative risk assessment [1, 2]. The knowledge of how parameter uncertainty influences the uncertainty in output is indispensible to direct the limited resources to the most influential parameters in terms of reducing uncertainty and improving system safety [3]. Global sensitivity analysis (GSA) [1, 4-6] is a useful technology to determine which parameters influence output the most when uncertainty in the parameters is propagated through the model. It can identify critical parameters and rank parameters with respect to reliability and risk [4]. Borgonovo [7] classified the GSA-based measures into three categories: 1) nonparametric techniques [8], 2) variance-based importance measures [9] and 3) moment-independent sensitivity indicators [3]. Essentially, GSA quantifies the contribution by individual parameters to the *overall* output uncertainty [10]. However, in the context of safety systems, we may be more interested in how the parameter uncertainty affects output uncertainty *that is relevant to system safety* (or equivalently, unsafety) [11], as discussed subsequently. Current techniques are exclusively focused on overall uncertainty, and safety-related (SR) uncertainty has largely been under-explored.

Safety systems are widely used in industry to reduce or prevent risk [11-13]. International standards like IEC 61508 [14] require especially for high safety applications a quantification of the achieved safety. In order to comply with this standard, the safety system has to be quantified to the “safety integrity level” (SIL). The IEC61508 standard discerns four SILs as shown in Table 1 [14]. The achieved SIL of a safety system can be obtained by calculating the average probability of failure on demand or safety probability of a dangerous failure per hour. However, in practice, uncertainty in model and/or parameters results in a probability distribution of system failure covering more than one SIL. This study is mainly focused on uncertainty in parameters, and thus model uncertainty is not discussed further. Fig. 1 shows a high integrity pressure protection system studied by Rouvroye [11], where the distribution of the failure probability encloses SIL1, SIL2 and SIL3 because of parameter uncertainty. Assume that $p_{\mathrm{SIL}x}$ is the upper bound under safety integrity level x (x=1, 2, 3, 4). Table 1 gives $p_{\mathrm{SIL1}} = 10^{-1}$, $p_{\mathrm{SIL2}} = 10^{-2}$, $p_{\mathrm{SIL3}} = 10^{-3}$ and $p_{\mathrm{SIL4}} = 10^{-4}$ for the low demand mode of system operation. For example, if SIL2 is required, the distribution in Fig. 1 can be divided into two parts. The safety part corresponds to failure probability $Y >= p_{\mathrm{SIL2}}$ and unsafety refers to the region where $Y < p_{\mathrm{SIL2}}$. Clearly, a small region of unsafety is desired for the safety system. In this paper, we consider how the parameter uncertainty influences the uncertainty of the SIL (equivalently the unsafety region as given in Fig. 1). This influence, once properly quantified, is an important indicator to rank the importance of system parameters in terms of achieved integrity.

Table 1 Safety integrity levels according to the IEC 61508 standard.

SIL	Low demand mode (average probability of failure on demand)	High demand or continuous mode (probability of a dangerous failure per hour)
4	10^{-5}~10^{-4}	10^{-9}~10^{-8}
3	10^{-4}~10^{-3}	10^{-8}~10^{-7}
2	10^{-3}~10^{-2}	10^{-7}~10^{-6}
1	10^{-2}~10^{-1}	10^{-6}~10^{-5}

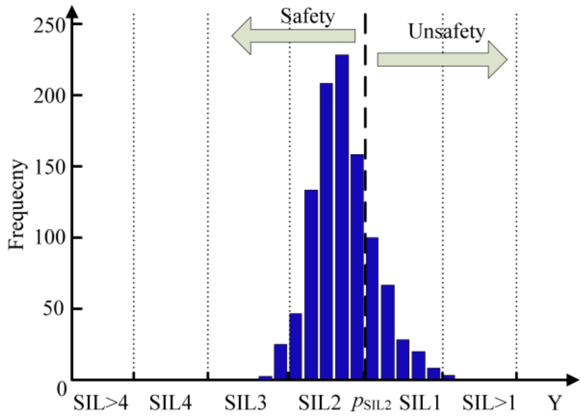


Fig.1 The distribution of probability of failure on demand.

As GSA techniques focus on the overall uncertainty of the model output, they are not suitable to measure SR uncertainty. In this work, we analyze how this issue can be addressed. We discuss the relationship between these two types of uncertainty, and propose four methods to handle SR uncertainty from different perspectives. The first method is based on the principle of reduction in the SR uncertainty if uncertainty in one parameter is eliminated. The second method evaluates the mean effect of parameter uncertainty on SR uncertainty. The third method assesses the rate of change in system unsafety by changing parameter uncertainty. The fourth method identifies which parameter's uncertainty influences the SR uncertainty the most in the view of variance. The proposed methods are applied to three systems models in comparison with GSA. The results highlight the need of the proposed measures when SR uncertainty is considered.

The remainder of the paper is organized as follows. Section 2 briefly reviews GSA and discusses the difference between overall uncertainty and SR uncertainty. Section 3 proposes four methods to measure the SR uncertainty. In Section 4, three examples are provided to illustrate the properties of the proposed methods when compared with GSA indicators. Section 5 concludes the paper.

2. Overall uncertainty and safety-related uncertainty

2.1. Assessing overall uncertainty through global sensitivity analysis

Let Y be the output of a system model $g(X)$ and $X = (X_1, X_2,\ldots,X_n)$ be a set of input parameters. The overall uncertainty links the uncertainty about X_i with the uncertainty about Y, which encloses the entire distribution of the model output Y [10]. GSA is an effective tool to assess the overall uncertainty due to parameter uncertainty. GSA provides a certain measure that quantifies the impact of parameters on system output. Various measures have been proposed in the literature [1, 3, 15, 16] and they may be classified into three categories [7]: 1) Non-parametric techniques; 2) Variance-based importance measure; and 3) Moment-independent sensitivity indicators.

The first category is based on non-parametric techniques that usually depend on the system model. For example, regression-based methods are appropriate when the system output is a linear function of the inputs [1]. These model-dependent methods are not discussed further; more details may be found in [1, 15, 16].

The variance-based importance measures consider the entire range of variation of the parameter and identify the contribution of individual parameters and their interactions. The variance-based measures are independent of the system model under study. A widely used measure due to Iman and Hora [9, 17] is

$$\mathrm{IH}_i = V[Y] - E\left\{V\left[Y\middle|X_i\right]\right\} = V\left\{E\left[Y\middle|X_i\right]\right\} \tag{1}$$

where V[Y] is the variance of the model output Y, and E{V[$Y|X_i$]} is the conditional expectation of the variance of Y with respect to the i-th parameter X_i. IH$_i$ quantifies the expected reduction in output variance if uncertainty in X_i is eliminated. The ranking of the importance of parameters based on IH$_i$ is the same as that based on the first order sensitivity index [18]. Clearly, the variance-based methods rely on a specific moment of the output distribution.

The third category of GSA is the moment-independent sensitivity indicators. These measures investigate the influence of parameter uncertainty on the entire output distribution without reference to a specific moment of the output [1]. Among this category, CHT$_i$ and δ_i are two important measures introduced by Chun et al. [3] and Borgonovo [1], respectively. The measure CHT$_i$ is defined by

$$\mathrm{CHT}_i = \frac{\left(\int_0^1 [P_t^i - P_t]^2 dt\right)^{1/2}}{E(Y)} \tag{2}$$

where P_t^i is the t-th quantile of a cumulative distribution function (CDF) for the "base case", P_t is the t-th quantile of a CDF for the "sensitivity case" and $E(Y)$ is the mean of output distribution for the "base case". The base case refers to the situation where the output distribution $f_Y(y)$ is obtained with all the parameter distributions being set to their nominal distributions, whereas in the sensitivity case the output distribution $f_{Y|X_i}(y)$ is obtained by changing the distribution of parameter X_i according to a certain strategy [3]. CHT$_i$ is essentially the metric distance in terms of quantiles between the base and sensitivity cases.

The measure δ_i is defined by

$$\delta_i = \frac{1}{2} E_{X_i}[s(X_i)] \tag{3}$$

with

$$s(X_i) = \int \left| f_Y(y) - f_{Y|X_i}(y) \right| \mathrm{d}y \tag{4}$$

where $f_Y(y)$ is the density function of Y and $f_{Y|X_i}(y)$ is the conditional density function of Y given X_i. This measure denotes the expected shift between the distribution of output Y and conditional distribution of output Y given X_i. The main difference the two measures is that CHT$_i$ requires to hypothesize a “sensitivity case” as discussed previously, while δ_i does not.

Subsequently, the measures of IH$_i$ and δ_i will be used to assess overall system uncertainty, against which the proposed SR uncertainty measures will be compared.

2.2. Safety-related uncertainty

When we consider safety systems, besides the overall uncertainty we are also interested in SR uncertainty, i.e. how the achieved safety level is affected by parameter uncertainty. For example, safety systems that need to comply with the IEC 61508 should reach a certain SIL and thus be considered safe (otherwise they are considered unsafe). Usually, a point estimate (i.e. average) of the probability of failure on demand (or safety probability of a dangerous failure per hour) is used to judge whether the system achieves the required SIL. However, when the uncertainty of parameters is considered, the probability of failure on demand itself becomes a random variable, and its distribution may enclose more than one SIL. For example in Fig. 1, if SIL-2 is the required safety level, the region to the right of the dashed line (i.e. the failure probability $Y > p_{\mathrm{SIL2}}$) is considered unsafety. For safety systems, a minimal unsafety region is desired. The primary objective of this paper is to identify which parameter influences the unsafety region the most. The uncertainty of the unsafety region due to parameter uncertainty is called SR uncertainty.

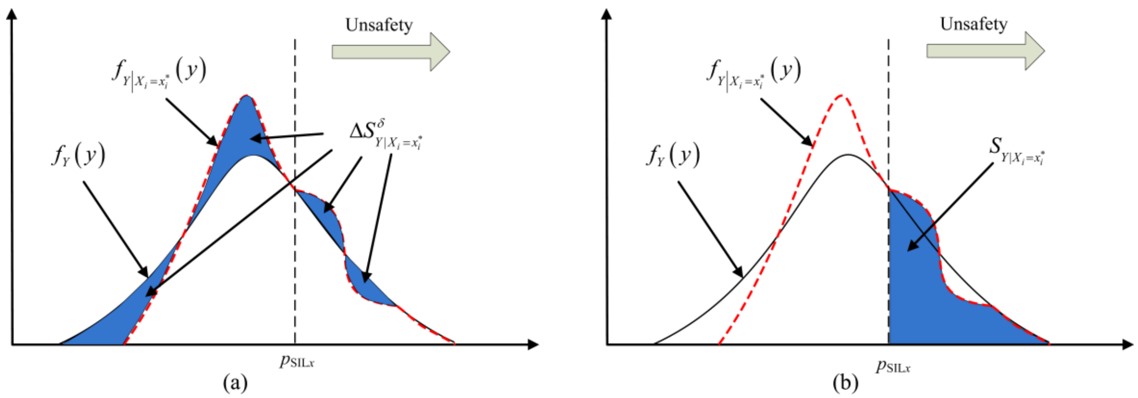


Fig.2 The density $f_Y(y)$ (solid) and conditional density $f_{Y|X_i=x_i^*}(y)$ (dashed).

Fig. 2 illustrates the fundamental concept of SR uncertainty. The δ_i measure from GSA (Eq.(3)) calculates the overall difference between $f_Y(y)$ and $f_{Y|X_i=x_i^*}(y)$ (the shaded area in Fig. 2 (a)), while the SR uncertainty concerns with the change of unsafety probability when the uncertainty in X_i is eliminated. As shown in Fig. 2 (b), if given $X_i = x_i^*$, the *size* of conditional unsafety region $S_{Y|X_i=x_i^*}$ equals to the original unsafety region, we say that the parameter X_i in the value x_i^* has no contribution to SR uncertainty. Moreover, it is possible that SR uncertainty will increase by reducing the uncertainty of certain parameters, which is impossible for overall uncertainty. These parameters have adverse effect on reducing SR uncertainty and should be ranked as the least important to SR uncertainty, since the existence of their uncertainty is desired for reduced system unsafety. Therefore, no effort may be needed to reduce these parameters’ uncertainty.

2.3. Overall uncertainty and SR uncertainty may rank the importance of parameters differently

Since GSA is focused on the overall uncertainty while SR uncertainty is only concerned with the uncertainty that is directly related to achieved safety, these two methods may differ in ranking the importance of parameters. Fig. 3 illustrates an example where two parameters, X_1 and X_2, are considered.

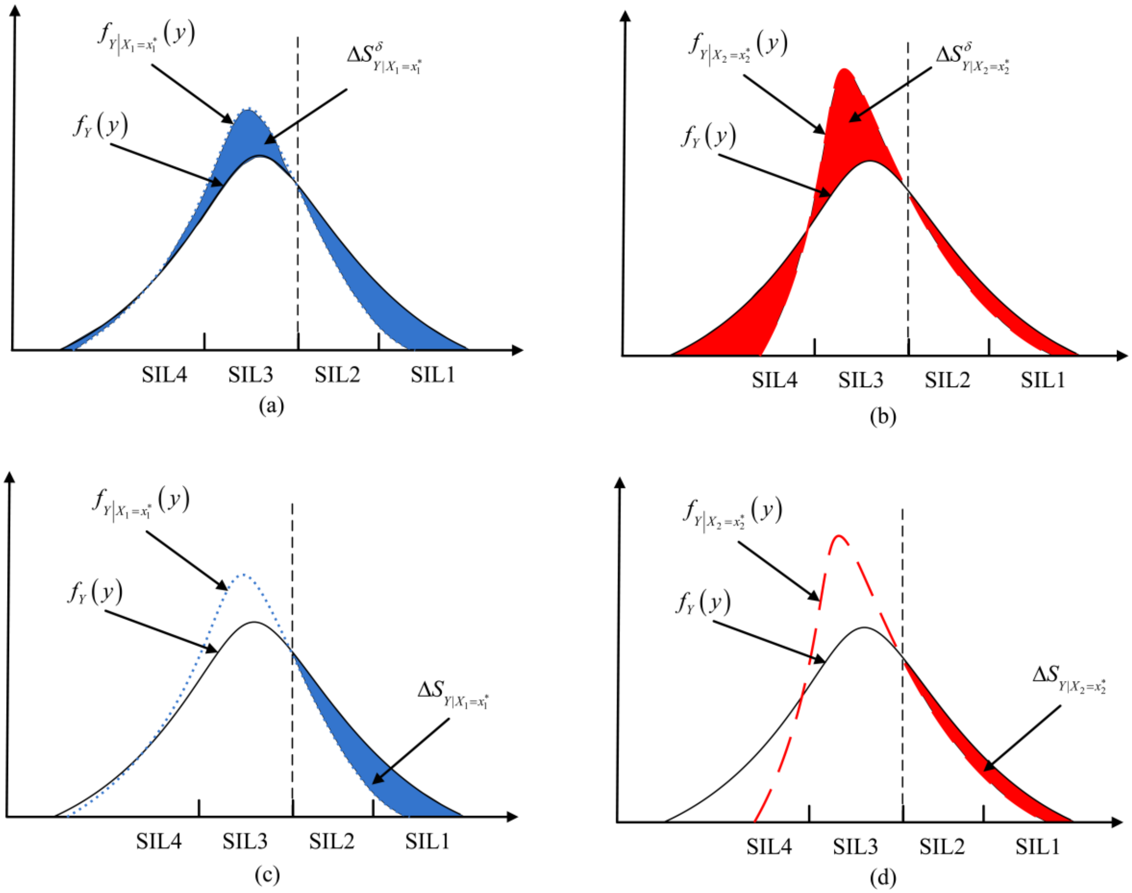


Fig.3 The density $f_Y(y)$ and conditional density $f_{Y|X_i=x_i^*}(y)$, i = 1,2. (a)(b): overall uncertainty; (c)(d): SR uncertainty.

In Fig. 3, the shaded area $\Delta S^{\delta}_{Y|X_i=x_i^*}$ is the shift between the two densities $f_Y(y)$ and $f_{Y|X_i=x_i^*}(y)$, i=1,2. A comparison between Fig. 3(a) and (b) show $\Delta S^{\delta}_{Y|X_1=x_1^*} < \Delta S^{\delta}_{Y|X_2=x_2^*}$, and the measure by Borgonovo [1] indicates $\delta_1 < \delta_2$, i.e. X_2 is more influential than X_1. However, the SR uncertainty measure, as shown in Fig. 3(c) and (d), shows $\Delta S_{Y|X_1=x_1^*} > \Delta S_{Y|X_2=x_2^*}$, i.e. the shift between $f_Y(y)$ and $f_{Y|X_1=x_1^*}(y)$ is greater than the shift between $f_Y(y)$ and $f_{Y|X_2=x_2^*}(y)$ with regard to system unsafety. Hence, X_1 is concluded to be more influential than X_2. Two completely opposite results may be obtained, depending on either overall uncertainty or SR uncertainty is considered. In practice, GSA techniques become inappropriate when SR uncertainty is of concern. Next, the methods to quantify the SR uncertainty are proposed.

3. Safety-related uncertainty measures

The relevant notations used in this paper are as follows.

(1) . $\underline{X} = (X_1, X_2, \ldots, X_n) \in R^n$ is the set of uncertain input parameters.

(2). $Y = g\left(\underline{X}\right), g\left(\underline{X}\right): E \subseteq R^n \to R$ is the function relationship between output Y and input parameters $\underline{X}$, i.e. the known system model.

(3). $\underline{x} = \left(x_1, x_2, \ldots, x_n\right)$ is a realization of $\underline{X}$.

(4). $f_{\underline{X}}\left(\underline{x}\right)$ is the joint density of $\underline{X}$.

(5). $f_{X_i}\left(x_i\right)$ is the marginal density of x_i.

(6). $f_Y(y)$ is the density function of the model output Y.

(7). $f_{Y|X_i}(y)$ is the conditional density of Y given one parameter X_i being fixed.

(8). $p_{\mathrm{SIL}x}$ is the upper bound under safety integrity level x (x=1, 2, 3, 4). Table 1 gives $p_{\mathrm{SIL1}}=10^{-1}$, $p_{\mathrm{SIL2}}=10^{-2}$, $p_{\mathrm{SIL3}}=10^{-3}$ and $p_{\mathrm{SIL4}}=10^{-4}$ for the low demand mode of system operation.

3.1. Method 1

Assume that SILx is the required safety integrity level. Let S be the failure probability of safety system above $p_{\mathrm{SIL}x}$:

$$S_Y = \int_{p_{SILx}}^{\infty} f_Y\left(y\right) dy \tag{5}$$

Further, let $S_{Y|X_i=x_i^*}$ be the failure probability of safety system above $p_{\mathrm{SIL}x}$ given $X_i = x_i^*$:

$$S_{Y|X_i=x_i^*} = \int_{p_{SILx}}^{\infty} f_{Y|X_i=x_i^*}\left(y\right) dy \tag{6}$$

Then, the reduction of SR uncertainty due to observing the i-th parameter may be measured by:

$$\mathrm{M1}_i = \frac{S_Y - S_{Y|X_i=x_i^*}}{S_Y} \tag{7}$$

In Eq.(7), x_i^* may simply be taken as the expected value of X_i, i.e. x_i^* =E(X_i). Note that when considering SR uncertainty, the safety system should satisfy the required SILx (i.e. E[Y]$\leq$ $p_{\mathrm{SIL}x}$). Method 1 quantifies the change in the probability of unsafety if the uncertainty in X_i is eliminated.

Since S_Y and $S_{Y|X_i=x_i^*}$ are the failure probabilities, $S_Y \in [0,1]$ and $S_{Y|X_i=x_i^*} \in [0,1]$, and thus M1$_i$ takes values in (-∞,1]. M1$_i$=1 means complete reduction of the system unsafety (the shaded area in Fig. 4(a)) if the uncertainty in X_i is eliminated and M1$_i$=0 indicates that the uncertainty of X_i has no effect on the system unsafety. In contrast, M1$_i$< 0 denotes increase in the system unsafety (the shaded area in Fig. 4(b)) if the uncertainty in X_i is eliminated. In this case, we may prefer to keep the existing uncertainty in X_i. Hence, the parameter with the highest M1$_i$ value is ranked as the most influential as far as reducing unsafety probability is concerned.

One natural extension of M1$_i$ is to replace $S_{Y|X_i=x_i^*}$ by the expectation of $S_{Y|X_i}$ with respect to X_i, giving rise to a new measure $\mathrm{M1}_i^{'}$:

$$\mathrm{M1}_i^{'} = \frac{S_Y - \int f_{X_i}\left(x_i\right) \int_{p_{SILx}}^{\infty} f_{Y|X_i}\left(y\right) dy dx_i}{S_Y} = \frac{S_Y - E[S_{Y|X_i}]}{S_Y} \tag{8}$$

In analogous to M1$_i$, $\mathrm{M1}_i^{'}$ takes values in (-∞,1] and its magnitude quantifies the influence of parameter uncertainty on the system unsafety. The sign of $\mathrm{M1}_i^{'}$ denotes the “direction” of the influence, also similar to M1$_i$. Therefore, the parameter with the highest $\mathrm{M1}_i^{'}$ value is ranked as the most influential with regard to SR uncertainty.

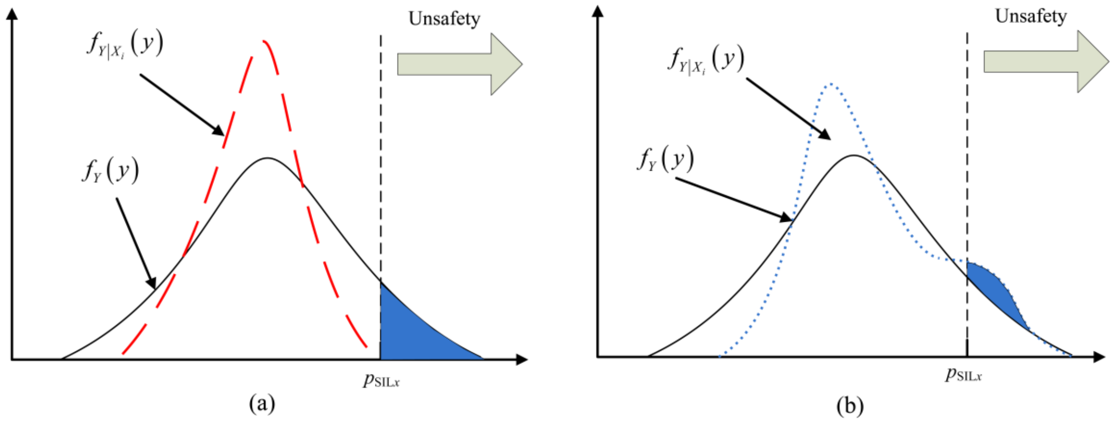


Fig.4 The reduction in the probability of unsafety with eliminated uncertainty in X_i.

3.2. Method 2

The definition of Method 2 is given by

$$\mathrm{M2}_i = \frac{V(X_i)}{S_Y}\frac{\partial S_Y}{\partial V(X_i)} \tag{9}$$

This method measures the rate of change in system unsafety due to the change in the variance of X_i. If $\mathrm{M2}_i > 0$, reducing the uncertainty of X_i will reduce system unsafety S_Y. On the contrary, a negative $\mathrm{M2}_i$ suggests an increase of system unsafety by reducing the uncertainty of X_i. Therefore, the parameter with the highest $\mathrm{M2}_i$ value is ranked as the most influential with regard to SR uncertainty.

3.3. Method 3

The third method proposed in this paper is a variance-based measure, and the definition is given by

$$\mathrm{M3}_i = V(X_i)\frac{\partial V(S_{Y|X_i})}{\partial V(X_i)} \tag{10}$$

where $V(S_{Y|X_i})$ is variance of system unsafety with respect to X_i. This method measures the change in the variance of system unsafety due to the change in the variance of X_i. It should be noted that $\mathrm{M3}_i$ measures the absolute change in the *variance* of system unsafety by varying the uncertainty in X_i, while $\mathrm{M2}_i$ measures the relative change in system unsafety by changing the uncertainty in X_i. If $\mathrm{M3}_i > 0$ (or $\mathrm{M3}_i < 0$), the reduction in uncertainty of X_i will decrease (or increase) the uncertainty of S_Y. Thus, the parameter with the largest $\mathrm{M3}_i$ value poses the greatest influence on the uncertainty of S_Y.

3.4. Numerical computation

The proposed SR uncertainty measures are computed using Monte Carlo (MC) simulation. For each simulation run, m MC samples are generated from the distribution of input parameters $f_{\underline{X}}(\underline{x})$, based on which the output distribution $f_Y(y)$, and thus the system unsafety in Eq.(5) can be approximated. To calculate $S_{Y|X_i=x_i^*}$, we may replace the i-th parameter of all the m samples by E(X_i), followed by the computation of the conditional output distribution and thus its integration as in Eq.(6). Then, $\mathrm{M1}_i$ can be obtained for each input parameter. Similar procedure can be used for obtaining $\mathrm{M1}_i^{'}$.

The partial derivatives in Methods 2 and 3 are approximated by finite difference. Specifically, the variance of X_i is reduced by a small amount (and denoted by $X_i^{'}$):

$$V(X_i) = V(X_i^{'}) + \alpha V(X_i) \tag{11}$$

and the measures are calculated as follows:

$$\mathrm{M2}_i = \frac{V(X_i)}{S_Y}\frac{\partial S_Y}{\partial V(X_i)} \approx \frac{V(X_i)}{S_Y}\frac{S_Y - S_{Y'}}{\alpha V(X_i)} \tag{12}$$

$$\mathrm{M3}_i = V(X_i)\frac{\partial V(S_{Y|X_i})}{\partial V(X_i)} \approx V(X_i)\frac{V(S_{Y|X_i}) - V(S_{Y|X_i'})}{\alpha V(X_i)} \tag{13}$$

where $S_{Y'}$ and $V(S_{Y|X_i'})$ are respectively system unsafety and the variance of system unsafety with the variance of X_i being reduced by $100\alpha\%$.

Normally, in finite-difference method where the function to be differentiated is deterministic, a small value for α (yet not small enough to be comparable with the computer’s numeric precision) is desired, such as 0.001. However, Eqs. (12) and (13) are stochastic functions, and thus using such a small α is numerically unstable unless an extremely large number of MC samples are used. In this study, a relatively large value α=0.2 is adopted based on empirical study, which will be further discussed along with the results in the next section.

In addition, the sample size is taken as m=10000. To ensure the robustness of the MC method, N=100 replicated simulations are performed and the average values of the importance measures are reported. The choice of these settings gives reliable results, and it is consistent with those reported in the literature [19].

4. Examples

Three examples are selected to demonstrate the application of the proposed methods, including two simple models and a two-out-of-three system.

4.1. Example 1: a simple example for illustration

To understand the relationship between the proposed methods and GSA, consider a simple example given below

$$Y = (X_1 + X_2)/11 \tag{14}$$

where the uncertainty of X_1 and X_2 are given by the following probability density function:

$$f_{X_1}(x_1) = Beta(x_1, 2, 16) \tag{15}$$

$$f_{X_2}(x_2) = Beta(x_2, 16, 2) \tag{16}$$

The distributions of X_1 and X_2 are positively and negatively skewed respectively as shown in Fig. 5. The corresponding distribution of model output Y is shown in Fig. 6. The statistical properties of the parameters and the model output are summarized in Table 2.

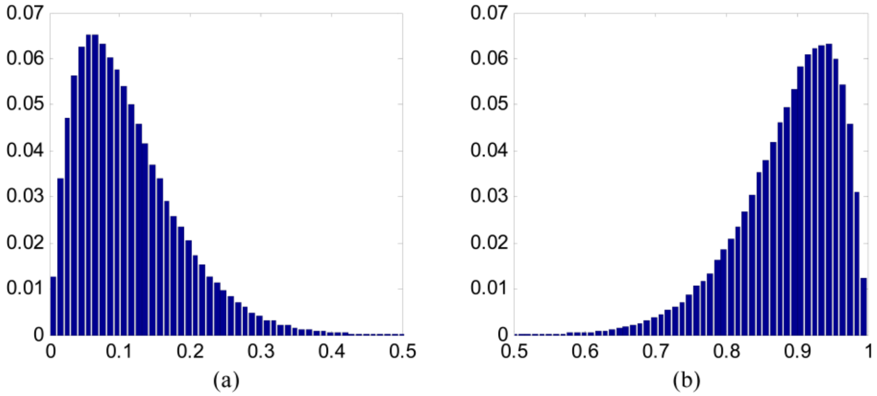


Fig.5 The distribution of parameters: (a) X_1; (b) X_2.

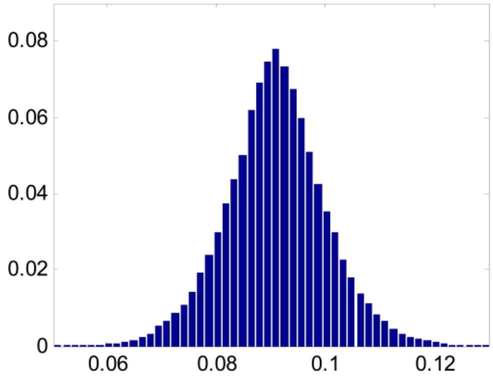


Fig.6 The distribution of model output *Y*.

Table 2 Statistical properties of the parameters and the model output.

	Distribution	Mean	Standard Deviation
X_1	Beta	0.11	0.72×10^{-1}
X_2	Beta	0.89	0.72×10^{-1}
Y		0.09	0.93×10^{-2}

Assume that the required SIL is level 1 and the failure probability greater than $p_{\mathrm{SIL1}}=10^{-1}$ is considered unsafe. Table 3 shows the results of M2$_i$ and M3$_i$ when varying the parameter α in the finite difference method (Eqs. (12)(13)). The last column in the table refers to the percentage that the rankings (from N=100 repeated MC simulations) are consistent with the final ranking (from the average of these 100 repetitions). A larger percentage indicates a more stable calculation. Clearly, when a small α (0.001 or 0.01) is used, finite difference does not give stable approximation to the partial derivatives. This phenomenon can be rectified, in theory, by using a very large number of MC samples. Nevertheless, it is practically more desirable to choose a relatively large α to achieve reasonable calculation while maintaining a low computational cost. Based on the results in Table 3, α=0.2 appears to be a good choice and is adopted for this example. Furthermore, the same procedure has been carried out for all the three examples presented in this paper and the results all supported the choice of α=0.2 (details not reported for the rest two examples for the sake of conciseness).

Table 3 SR uncertainty measures (M2$_i$ and M3$_i$) calculated by varying α.

	α	X_1		X_2		Percentage
		Results	Ranking	Results	Ranking	
M2$_i$	0.001	0.70	1	-1.00	2	58%
	0.01	124.27	1	1.25	2	65%
	0.1	0.36	1	0.21	2	80%
	0.2	0.42	1	0.29	2	100%
	0.3	0.44	1	0.30	2	100%
M3$_i$	0.001	0.50	1	0.44	2	62%
(10^{-1})	0.01	-3.40	2	0.18	1	68%
	0.1	0.41	1	0.12	2	100%
	0.2	0.49	1	0.12	2	100%
	0.3	0.50	1	0.12	2	100%

Besides the four proposed measures, two GSA indicators (δ and IH) are also calculated and the results are shown in Table 4.

Table 4 Uncertainty importance measures and their ranking (bracketed, "E" refers to equal ranking).

Parameter	δ_i		$\mathrm{IH}_i\,(10^{-4})$		$\mathrm{M1}_i$		$\mathrm{M1}_i^{'}$		$\mathrm{M2}_i$		$\mathrm{M3}_i\,(10^{-1})$	
X_1	0.35	(E)	0.43	(E)	0.90	(1)	0.00	(E)	0.42	(1)	0.49	(1)
X_2	0.35	(E)	0.43	(E)	0.34	(2)	0.00	(E)	0.29	(2)	0.12	(2)

Table 4 shows that X_1 and X_2 are equally important according to δ_i and IH$_i$. The two GSA measures are unable to distinguish the importance of the two parameters, so is the proposed $\mathrm{M1}_i^{'}$ measure. However, M1$_i$, M2$_i$ and M3$_i$ suggest that X_1 is more influential than X_2 with regard to SR uncertainty. M1$_i$ indicates that if the uncertainty of X_1 (X_2) is eliminated, the system unsafety region is reduced by 90% (34%). M2$_i$ denotes higher relative reduction of system unsafety by reducing the variance of X_1 (0.42) than that by reducing the variance of X_2 (0.29). M3$_i$ also supports the conclusion that X_1 is more important than X_2 in the view of SR uncertainty. Note that $\mathrm{M1}_i^{'}$ cannot distinguish X_1 and X_2 in this example because $S_Y \approx E\left(S_{Y|X_i}\right)$.

The importance ranking may be potentially used to improve the system safety by reducing parameter uncertainty. Following the ranking based on SR uncertainty, the uncertainty of X_1 may be reduced. As an example, suppose that the standard deviation of X_1 is reduced from 0.72×10^{-1} to 0.23×10^{-1}, and the original and reduced distribution of model output Y are shown in Fig. 7(a). For comparison, we may choose to reduce the standard deviation of X_2 from 0.72×10^{-1} to 0.23×10^{-1} instead of changing that of X_1, and the original and reduced distribution of model output Y are shown in Fig. 7(b).

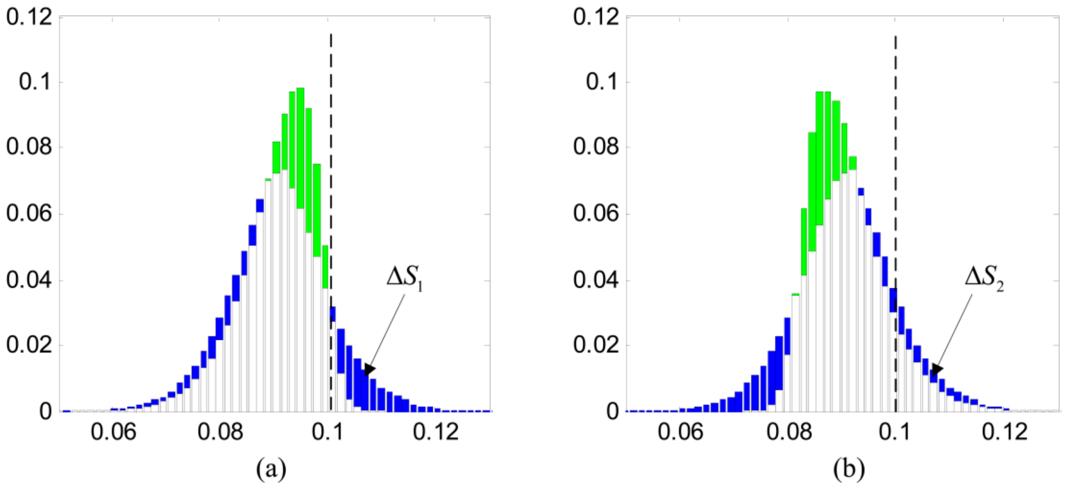


Fig.7 The distribution of model output Y with reduced uncertainty of (a) X_1, (b) X_2.

As shown in Fig. 7(a), the white and blue bars compose the original distribution of model output Y, while the white and green bars represent the distribution of Y with reduced uncertainty of X_1. The reduced SR uncertainty in case 1 is ΔS_1 (blue bars on the right of the dashed line in Fig. 7(a)). Similarly, ΔS_2 in Fig. 7(b) is the reduced unsafety probability in case 2. Clearly $\Delta S_1 > \Delta S_2$, suggesting that reducing the uncertainty in X_1 is more effective than reducing the uncertainty in X_2 towards reducing the SR uncertainty. In comparison, the overall shift (the blue bars and green bars) in the two cases are the same, and this is why the GSA measures, δ_i and IH$_i$ that consider overall uncertainty of the system, are unable to distinguish the two input parameters. This example also indicates that the $\mathrm{M1}_i^{'}$ measure may not be appropriate to assess SR uncertainty.

4.2. Example 2: two components in series

The previous example is extended to a system with two components in series shown in Fig. 8.

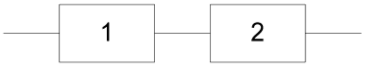


Fig.8 System with two components in series.

Assume the failure probability of the two components are $X_1/11$ and $X_2/11$, respectively. Hence, the failure probability of the system is

$$Y = \frac{X_1 + X_2}{11} - \frac{X_1 X_2}{121} \tag{17}$$

Using the same parameter distribution as in Table 2, the results are shown in Table 5.

Table 5 Uncertainty importance measures and their ranking (bracketed, "E" refers to equal ranking).

Parameter	δ_i	IH$_i$ (10^{-4})	M1$_i$	$\mathrm{M1}_i^{'}$	M2$_i$	M3$_i$ (10^{-1})
X_1	0.33 (2)	0.36 (2)	1.00 (1)	0.00 (E)	0.55 (1)	0.45 (1)
X_2	0.36 (1)	0.41 (1)	0.40 (2)	0.00 (E)	0.34 (2)	0.10 (2)

Table 5 shows that M1$_i$, M2$_i$ and M3$_i$ give the same ranking for the two parameters, that the uncertainty in X_1 is more influential on the SR uncertainty than that in X_2 is. GSA measures give the opposite conclusion by considering the overall system uncertainty. Again, $\mathrm{M1}_i^{'}$ still cannot distinguish X_1 and X_2 in this example, because we observed that $S_Y \approx E\left(S_{Y|X_i}\right)$. The importance of X_1 on SR uncertainty, in comparison with X_2, was also verified (detailed not reported here) by reducing the input uncertainty and observing the change of unsafety probability, similar to the method presented for Example 1.

4.3. Example 3: two out of three (2oo3) system

In this example, a more practical system with a 2oo3 (two-out-of-three) architecture, which is widely used in industry, is considered [20]:

$$\begin{aligned} Y_{PFD} = {} & 3T_1\left(\lambda_D(1-\beta)(1-DC_D)\right)^2 (T_1/3 + MTTR) \\ & + \lambda_D(1-DC_D)(T_1/2 + MTTR)(6\lambda_D DC_D + \beta) \\ & + 3\left(\lambda_D DC_D MTTR(1-\beta_D)\right)^2 + \beta_D \lambda_D DC_D MTTR \end{aligned} \tag{18}$$

Table 6 and the values are within the recommend ranges of IEC 61508 standard. The proof-test interval T$_1$ can be fixed to one year according to [14]. The other parameters are assumed to follow the conventional lognormal distribution [11], whose mean and variance can be obtained by converting the range in Table 6 (See Appendix A for detail). Subsequently, MC simulation is used to calculate the output distribution and the importance measures. The mean of the output distribution, $f_{Y_{PFD}}(y)$, is 5.6×10^{-4}. based on which we assume that the safety system requires SIL-3. The results of the five measures are shown in Table 7.

Table 6 The parameters used in the 2oo3 model.

Parameter	mean	Value
λ_D (/h)	Dangerous failure rate	4×10^{-6}~8×10^{-7}
β	Common cause factor for dangerous undetected failures	0.02~0.2
β_D	Common cause factor for dangerous detected failures	0.01~0.1
DC_D	Safe diagnostic coverage coefficient	0.2~0.9
$MTTR$ (h)	Mean Time to Restoration	4~24
T_I (y)	Proof-test interval	1

Table 7 Uncertainty importance measures and their ranking.

Parameter	δ_i (10^{-1})		IH$_i$ (10^{-8})		M1$_i$ (10^{-1})		$\mathrm{M1}_i^{'}$ (10^{-3})		M2$_i$ (10^{-1})		M3$_i$ (10^{-2})	
λ_D	2.28	(1)	9.74	(1)	4.09	(1)	0.96	(2)	3.97	(1)	3.19	(1)
β	1.87	(3)	7.05	(2)	2.00	(2)	0.46	(3)	2.83	(2)	1.92	(2)
β_D	0.00	(5)	0.00	(5)	0.00	(5)	0.04	(5)	0.00	(5)	0.00	(5)
DC_D	2.22	(2)	3.54	(3)	1.66	(3)	3.37	(1)	0.19	(3)	0.41	(3)
$MTTR$	0.01	(4)	0.00	(4)	0.00	(4)	0.13	(4)	0.02	(4)	0.00	(4)

Table 7 shows that M1$_i$, M2$_i$, M3$_i$ and IH$_i$ (hereafter the "four measures") give the same ranking. λ_D ranks 1st for all the measures except $\mathrm{M1}_i^{'}$. β ranks 2nd according to the "four measures" while it ranks 3rd according to δ_i and $\mathrm{M1}_i^{'}$. DC_D ranks 3rd according to the "four measures" while it ranks 2nd based on δ_i and 1st based on $\mathrm{M1}_i^{'}$. For all the measures, *MTTR* ranks 4th and β_D ranks 5th, and their values are far less than the values of other parameters. Hence, the effect on both overall and SR uncertainty due to uncertainty of *MTTR* and β_D is negligible. In the view of the most important parameter, the rank given by $\mathrm{M1}_i^{'}$ is very different from those given by other measures. It appears that $\mathrm{M1}_i^{'}$ can only identify the group of the most influential parameters (DC_D, λ_D and β), but it cannot distinguish them in detail. As a result, $\mathrm{M1}_i^{'}$ is not recommended to measure SR uncertainty.

Above discussion also shows that the proposed methods (expect $\mathrm{M1}_i^{'}$) and the two GSA measures give similar results, though they focus on different aspects of system uncertainty. This is because the effect of parameter uncertainty with regard to overall uncertainty and SR uncertainty is similar in the example.

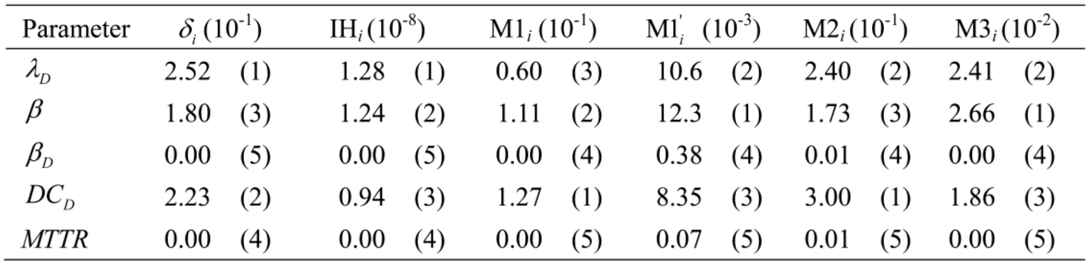
To further illustrate the importance of SR uncertainty, the probability distributions of two parameters, β and DC_D, are modified to beta distribution with the following density functions:

$$f_\beta\left(x\right)=Beta\left(x,2,16\right) \tag{19}$$

$$f_{DC_D}\left(x\right)=Beta\left(x,1.2,1.8\right) \tag{20}$$

which are heavily skewed when compared with the original log-normal distribution. By keeping all other settings unchanged, the results are given in Table 8.

Table 8 Uncertainty importance measures and their ranking (β and DC_D are changed to conform to beta distributions).



Parameter	δ_i (10^{-1})	IH$_i$ (10^{-8})	M1$_i$ (10^{-1})	M1$'_i$ (10^{-3})	M2$_i$ (10^{-1})	M3$_i$ (10^{-2})
λ_D	2.52 (1)	1.28 (1)	0.60 (3)	10.6 (2)	2.40 (2)	2.41 (2)
β	1.80 (3)	1.24 (2)	1.11 (2)	12.3 (1)	1.73 (3)	2.66 (1)
β_D	0.00 (5)	0.00 (5)	0.00 (4)	0.38 (4)	0.01 (4)	0.00 (4)
DC_D	2.23 (2)	0.94 (3)	1.27 (1)	8.35 (3)	3.00 (1)	1.86 (3)
$MTTR$	0.00 (4)	0.00 (4)	0.00 (5)	0.07 (5)	0.01 (5)	0.00 (5)

Table 8 shows that the ranking given by the proposed methods and the two GSA measures are different with regard to the most and least important parameters. DC_D ranks 1st according to M1$_i$ and M2$_i$, while it ranks 2nd based on δ_i and 3rd by using IH$_i$, M1$'_i$ and M3$_i$. λ_D ranks 2nd according to M2$_i$, M1$'_i$ and M3$_i$ while it ranks 1st based on δ_i and IH$_i$, and 3rd based on M1$_i$. β ranks 3rd by δ_i and M2$_i$ while it ranks 2nd according to IH$_i$ and M1$_i$, and 1st based on M3$_i$. All the proposed SR uncertainty measures agree that *MTTR* is the least important while the two GSA methods give β_D the lowest rank.

It should be noted that the SR measures do not always agree with each other in terms of the exact ranking of parameters. This phenomenon is not surprising since these SR measures are defined from different perspectives. In practice, the most appropriate SR uncertainty measure is likely to depend on specific applications and thus should be carefully selected.

5. Conclusions

Traditionally, quantitative risk assessment has been focused on investigating how the uncertainty of input parameters affects that of system output in an overall sense. This paper introduces the concept of safety-related uncertainty and highlights its relevance for the analysis of safety systems. The conventional GSA that provides information about the overall uncertainty is inappropriate to measure SR uncertainty. Therefore, four new methods are developed in this paper to quantify and rank the impact of individual parameters on SR uncertainty, and they are demonstrated through the application to three examples. In the first two examples, the proposed SR uncertainty measures correctly rank the parameters with regard to achieved safety, while the GSA measures either are unable to distinguish the importance of the two parameters (example 1), or give the opposite conclusion by considering the overall uncertainty (example 2). In the third example, the proposed methods and GSA measures obtain inconsistent results in particular regarding the most and least important parameters when the distributions of β and DC_D are heavily skewed. The results indicate the need of the proposed measures when SR uncertainty is considered. Nevertheless, the measure M1$'_i$ appears to be incapable of assessing the parameters' importance appropriately in the studied examples.

Acknowledgements

This work is partially supported by Ministry of Railways of China (Scientific Research and Development Program No. 2008X003-C), and National Natural Science Foundation of China (Grant No. 60674064).

Appendix A. Converting data into lognormal distribution

In practice, data are often given in the form of a triplet (minimum, typical, maximum), duple (minimum, maximum), or even a point estimate [11]. Probabilistic analysis requires to convert such data into a certain distribution with required characteristics. This appendix explains how to convert data into lognormal distribution based on the results in [11].

The density function of lognormal distribution is given by:

$$f(x)=\frac{1}{x\sigma\sqrt{2\pi}}\exp\left(-\frac{1}{2\sigma^2}\left(\ln(x)-\ln(x_0)\right)^2\right) \tag{A.1}$$

The median of the lognormal distribution is x_0. The problem now is how to choose the parameters σ and x_0.

First, we discuss the form of triplet. Let *m*, *T* and *M* denote the minimum, typical and maximum values, respectively. In this case, m is defined by dividing the typical value by a certain factor *F* (*m*=*T*/*F*) and *M* is given by multiplying the typical value with the same factor (*M* = *T* × *F*). The following method can be used to determine σ and x_0.

1). Choose x_0 equal to the typical value *T*.

2). Choose σ in such a way that the probability for obtaining values between the minimum and the maximum is given by *P* (In Example 3 of this paper, *P* is taken as 0.95). This implies that σ is chosen so that :

$$P=\int_m^M \frac{1}{x\sigma\sqrt{2\pi}}\exp\left(-\frac{1}{2\sigma^2}\left(\ln(x)-\ln(x_0)\right)^2\right)dx \tag{A.2}$$

Define the auxiliary variable *z* as

$$z=\frac{1}{\sqrt{2}\sigma}\ln\left(\frac{x}{T}\right) \tag{A.3}$$

In addition, the definition of the Gaussian error function is

$$erf(x)=\frac{2}{\sqrt{\pi}}\int_0^x \exp\left(-t^2\right)dt \tag{A.4}$$

From Eqs. (A.2)(A.3)(A.4) we have

$$P=erf\left(\frac{1}{\sqrt{2}\sigma}\ln(F)\right) \tag{A.5}$$

Now σ can be calculated with the help of the inverse function of the error function

$$\sigma=\frac{\ln(F)}{\sqrt{2}inverf(P)} \tag{A.6}$$

The error function and its inverse function are available in many computation software packages, e.g. Matlab.

If the form of duple (minimum, maximum) is given, a similar approach can be followed by using

$$T=\sqrt{mM} \quad and \quad F=\sqrt{\frac{M}{m}} \tag{A.7}$$

References

[1] Borgonovo E. A new uncertainty importance measure. Reliability Engineering & System Safety. 2007;92:771-84.

[2] Apostolakis GE. How Useful Is Quantitative Risk Assessment? Risk Analysis. 2004;24:515-20.

[3] Chun M-H, Han S-J, Tak N-IL. An uncertainty importance measure using a distance metric for the change in a cumulative distribution function. Reliability Engineering & System Safety. 2000;70:313-21.

[4] Aven T, Nøkland TE. On the use of uncertainty importance measures in reliability and risk analysis. Reliability Engineering & System Safety. 2010;95:127-33.

[5] Helton JC. Uncertainty and sensitivity analysis techniques for use in performance assessment for radioactive waste disposal. Reliability Engineering & System Safety. 1993;42:327-67.

[6] Borgonovo E, Apostolakis GE, Tarantola S, Saltelli A. Comparison of global sensitivity analysis techniques and importance measures in PSA. Reliability Engineering & System Safety. 2003;79:175-85.

[7] Borgonovo E. Measuring Uncertainty Importance: Investigation and Comparison of Alternative Approaches. Risk Analysis. 2006;26:1349-61.

[8] Saltelli A, Marivoet J. Non-parametric statistics in sensitivity analysis for model output: A comparison of selected techniques. Reliability Engineering & System Safety. 1990;28:229-53.

[9] Iman RL. A Matrix-Based Approach to Uncertainty and Sensitivity Analysis for Fault Trees1. Risk Analysis. 1987;7:21-33.

[10] Anand FS, Realff MJ, Lee JH. A Risk based Approach to Estimate Key Uncertainties. Proceedings of the 9th International Symposium on Dynamics and Control of Process Systems, DYCOPS 2010, June 5, 2010 - July 7, 2010. Leuven, Belgium: Mayuresh Kothare, Moses Tade, Alain Vande Wouwer, llse Smets; 2010. p. 569-74.

[11] Rouvroye J. Enhanced markov analysis as a method to assess safety in the process. Technische Universiteit Eindhoven, Dutch;2001.

[12] Rouvroye JL, van den Bliek EG. Comparing safety analysis techniques. Reliability Engineering & System Safety. 2002;75:289-94.

[13] Torres-Echeverría AC, Martorell S, Thompson HA. Design optimization of a safety-instrumented system based on RAMS+C addressing IEC 61508 requirements and diverse redundancy. Reliability Engineering & System Safety. 2009;94:162-79.

[14] International Electrotechnical Commission.Functional safety of electrical/electronic/programmable electronic safety-related systems. . IEC 61508,Parts1-7,1st Ed,Geneva, Switzerland, 1998.

[15] Hora SC, Helton JC. A distribution-free test for the relationship between model input and output when using Latin hypercube sampling. Reliability Engineering & System Safety. 2003;79:333-9.

[16] Christopher Frey H, Patil SR. Identification and Review of Sensitivity Analysis Methods. Risk Analysis. 2002;22:553-78.

[17] Iman RL, Hora SC. A Robust Measure of Uncertainty Importance for Use in Fault Tree System Analysis. Risk Analysis. 1990;10:401-6.

[18] Homma T, Saltelli A. Importance measures in global sensitivity analysis of nonlinear models. Reliability Engineering & System Safety. 1996;52:1-17.

[19] Liu Q, Homma T. A new computational method of a moment-independent uncertainty importance measure. Reliability Engineering & System Safety. 2009;94:1205-11.

[20] Oliveira LF, Abramovitch RN. Extension of ISA TR84.00.02 PFD equations to KooN architectures. Reliability Engineering & System Safety. 2010;95:707-15.